Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2008 Proceedings

European Conference on Information Systems (ECIS)

2008

Defining Internal Control Objectives for Information Systems Security: A Value Focused Assessment

Sushma Mishra
Virginia Commonwealth University, mishras@vcu.edu

Gaurpreet Dhillon
Virginia Commonwealth University, gdhillon@vcu.edu

DEFINING INTERNAL CONTROL OBJECTIVES FOR INFORMATION SYSTEMS SECURITY: A VALUE FOCUSED ASSESSMENT

Mishra, Sushma, Virginia Commonwealth University, 301 W Main Street, Box 844000, Richmond, Virginia, USA, mishras@vcu.edu

Dhillon, Gurpreet, Virginia Commonwealth University, 301 W Main Street, Box 844000, Richmond, Virginia, USA, gdhillon@vcu.edu

Abstract

Internal controls play an important role in overall effectiveness of information systems security. A theoretical framework of means-fundamental objectives for internal controls in information systems security context is presented. Data was collected through in-depth interview of 52 IT managers about their values in defining internal controls. A total of 68 objectives are identified which are organized into 25 clusters of seven fundamental and 18 means objectives. The findings form the basis for further theoretical expositions in security governance area. The objectives also help in defining governance related policy initiatives.

Keywords: internal controls, values, value theory, value focused thinking, decision objectives

1 INTRODUCTION

Kirsch (2002) defines control as a set of mechanisms designed in order to motivate individuals to attain desired objectives. Controls are fundamental to all organizations (Scott 1995). It provides a mechanism to align organizational goals and aspirations with employee's capabilities, activities and performance. Internal controls for information systems security can also be viewed as the practices, procedures, policies and responsibility structures in an organization that help in managing risks and protecting information assets (Dhillon, 2001). Internal controls play an important role in information systems security in an organization. Many security breaches have occurred due to lack of proper internal control structure in organizations. Sarbanes-Oxley Act was enacted in response to public outcry about ineffective internal control assessment procedures in organizations leading to major lapses of security and governance. In the literature, effective internal controls have been suggested to ensure business process integrity, continuity and adequate security governance (Dhillon, 2001; Warkentin and Johnston 2006; Whitman 2003). Lack of effective controls can lead to various issues including security breaches or subversion of controls or employees. Inability to define effective controls therefore leads to security problems.

In this paper, we define value based internal control objectives for information systems security. Individual values play an important role in developing decision objectives (Catton, 1952; Keeney, 1992). Decision objectives, rooted in individual values, provide a deeper understanding of organizational initiatives in the decision context (Dhillon and Torkzadeh, 2006). Since individual values are important in developing objectives, in this paper we develop control objectives based on the values of the IT managers. Incorporating values of individuals in control objectives helps in three ways: First, objectives created with individual values help in grounding the controls in contextual factors. Second, the internal control objectives provide a theoretical framework for

more rigorous investigation in this area. Third, value driven control objectives help in aligning individual and organizational objectives. Such initiatives reduce the gap between management's philosophy about controls and employee's interpretation of the same.

Using value theory and value focused approach as the theoretical and methodological basis; a study is conducted to define internal control objectives, grounded in individual values of people, for information systems security. Following the introduction, rest of the paper is presented as follows. The next section presents a review of literature in controls, based on two dimensions: scope and target of controls. The following section discusses the theoretical and methodological stand of this research. In the fourth section, the empirical study is presented with the means-fundamental framework. In the fifth section, discussions are presented. The last section presents the conclusion.

2 LITERATURE REVIEW: NATURE OF CONTROLS

Information systems in organizations are conceptualized to be working at three levels in an organization and so does internal control management program (Dhillon, 2006). These levels are: *formal (*messages from all external parties are interpreted and communicated for effective operations of the organization, example business strategies, corporate board, financial planning, human resources and marketing planning*), informal (*means to support the formal systems example subgroups formed within organizations, belief system of employees, implicit knowledge about work procedures, power and politics equation amongst groups*)* and *technical (*presumes a formal system exists and automates parts of it, example includes information technology automating business process workflow*)*. Management of information systems has to be an integrated approach at all the three levels. Controls have to operate at all the levels simultaneously to ensure comprehensive information systems effectiveness.

Ouchi (1979) argues that design of organizational control mechanisms focuses on achieving cooperation among individuals having divergent objectives. Goal congruity is a central mechanism of control in an organization (Ouchi, 1980). Based on the scope of the control, there are three modes of control that work in different ways to achieve cooperation amongst people who share partially congruent objectives (Ouchi, 1979). The market mode of control acts through its ability to precisely measure and reward individual contributions. It is applicable to tasks that are accurately measurable. The second mode of control, Bureaucratic control relies on mixture of close evaluation of performance and reward. It is achieved through formal structure of organizations, which acknowledges the work and rewards through incentives. The third mode of controls, Clan control relies completely upon socialization process, which effectively eliminates goal incongruence through shared beliefs and objectives. Clan control attains cooperation by socializing individuals such that individual objectives align with organizational objectives.

Markets, bureaucracies and clans are three distinct mechanisms, which are present in differing degrees in any real organization (Ouchi, 1980). The design problem of defining the control objectives is of assessing the social and information characteristics of each division, department or task and analyzing what would be the scope of control that needs to be emphasized in each case (Ouchi, 1979). Conceptually, it can be argued that the three modes of controls (market, bureaucratic, clan) are similar to the three levels of management in an organization (technical, formal, informal) because of similar informational requirements in each (Kirsch, 2002; Ouchi, 1980). In our classification of controls, we use formal, informal and technical taxonomy for the sake of clarity.

Based on the attributes of the production process that control mechanisms are intended to influence or the target of controls, Cardinal et al (2004) suggest three forms of controls. These forms of controls are:

Input: Input controls are aimed at managing resources acquired by firms, which constitutes of resources such as human, financial and material (Cardinal et al, 2004). Input mechanisms involve aligning individuals with interest of firms through selection and training (Snell, 1992).

Behavioral: Behavioral control structures the transformation process of work (Snell, 1992). It is usually initiated top down in the form of articulated operating procedure. Behavioral controls require an understanding of business activities to manage tasks that transform inputs into outputs. These controls determine how work gets done in an organization (Cardinal et al, 2004).

Output: Controls used to manage products and services outcomes and regulate results of the process are called output controls (Cardinal et al, 2004). Output controls measure the results of the transformation process from input through behavioural to the end result. It encourages subordination discretion by focusing on desired result and not on the process of achieving the result (Snell, 1992).

The scope dimension of the controls highlights the levels of management where the controls can be placed or specified. The target dimension of the control specifies the stage of business process where a particular control is targeted. Based on the particular business process state (input, behavioral, output) where a control is placed, the role of the control can be defined. Both the dimensions are complimentary and combining them provides a detailed picture of the nature, scope and role of a control and how a control can guide action. Overall this conceptualization represents organizational controls as the following matrix. A nuanced understanding of control strategies in the context of information systems security is highlighted through this matrix of controls (Table 1). A discussion of the controls requirements along each of the row of the matrix is provided:

Technical controls: All the controls are technical in scope and are targeted at the different stages of the business processes. These controls targeted at input of informational resources within an organization are primarily based on data input methods such as document design, screen design, batch controls and validation of data input in the organization. Research in technical controls targeted at the business processes is concerned about issues pertaining to access controls models (Jaeger and Zhang, 2003; Iwaihara and Hayashi, 2007), architecture controls, and authorization mechanisms (Thompson et al, 2003; Ferrari et al, 2002). Technical controls targeted at information resources interacting with outside environment, revolves around batch output controls and distribution controls. Some of the specific controls include: encryption (Bellare and Kohno, 2004; Rogaway et al, 2003), cryptography (Rothe, 2002; Mayers, 2001), filters (Herlocker et al, 2004; Hofmann, 2004), sniffers (Bapna, 2003), back up and disaster recovery plans (Choy et al, 2000).

Formal controls: All controls are formal in scope and are targeted at the different stages of the business processes. The formal controls at the input level of formal security decision-making and the scope is organizational structure and management. Research in this area entails formal decision points such as security budgets (Gordon and Loeb, 2006; Bodin et al, 2005), risk assessment models (Tiwana and Keil, 2004; Iversen et al, 1999; Lewis et al, 2003) physical security and recruitment rules, security strategy (Langfield-Smith, 1997); Snell, 1992). Controls targeted at the process level of formal security methods includes standards (Siponen, 2006), policies, procedures, internal audit (Hogg, 1992; Hansen and Hill, 1989) and training (Aeran, 2006). Formal controls targeted at the output or results of formal security methods and its interaction with the environment and the scope is organizational structure and management. Research in this area includes compliance mechanisms (Aeran, 2006), external audit and governance efforts for legitimacy (Moultan and Cole, 2003: CISA Review Manual, 2004).

Informal controls: All the controls are informal in nature. Informal controls targeted at the input level of business process emphasizes the importance of values (Galloway, 1994; Dhillon and

Torzedeh, 2006), motivations (Nidumolu and Subramani, 2003), behavior (Klein, 1989), culture, trust (Hoffman et al, 2006, Das and Teng, 1998) and awareness issues (Siponen, 2001). Research in informal controls targeted at the business process level of the organization include informal responsibility and accountability expectations (Pierce et al, 2001; Dhillon, 2001), power and politics issues in security decision making. Research in controls targeted at output of business security decisions and its impact on the environment includes alignment of business and individual goals (Alavi et al, 1986) business continuity (Roberts, 2006) and identifying.

Table 1. Research in information systems security domain based on conceptual matrix

		Target of Control		
		Input 1	Behavioral 2	Output 3
Scope of Control	Technical 1	Different types of data input methods such as document design, data entry screen design, batch controls, validation of data input, instruction input	Controls of physical components, topological controls, channel access controls, architecture controls, Access control models, Authorization mechanisms	Batch output production and distribution controls, online output production and distribution controls, Encryption, Cryptography, Filters, Sniffers
	Formal 2	Application system processing controls, Risk assessment models, Security investment budgets, Physical security, Recruitment rules, Business strategy	Long term policy design, Procedures, Audit, Training	Compliance, security management, data resource management, operations management controls, quality controls, Back up, Disaster recovery
	Informal 3	Values, Motivations, Culture, Trust, Sense of ownership	Responsibility and Accountability structures	Individual and business goal alignment, Business continuity, awareness, control consciousness

The purpose of this control matrix is to understand the business requirements based on intersection of scope and target of control mechanisms. Internal control objectives, based on the business requirement of each cell should be able to reflect the security needs in that cell.

While the academic literature on controls focuses on aspects of classification and theoretical models developed models that help in implementing controls irrespective of their nature and scope. Control Objectives for Information and related technology (COBIT) is the most widely used framework for information systems controls and related good practices (ISACA, 2004). COBIT primarily guides organizations for better information technology governance, control structures and means of providing assurance. It divides IT processes into four domains and 34 broad control objectives through the entire business process cycle. Similarly there is the COSO framework. COSO stands for the "Committee of Sponsoring Organizations of the Treadway Commission," a non-profit commission that in 1992 established a common definition of internal controls. The COSO framework views internal controls as consisting of the following five interrelated components: *control environment* **(“**setting the tone” of the organization or the broad ethical values of the management), *risk assessment* **(**process of identifying and mitigating risk activities in the organization), *control activities* (identifies internal control activities to mitigate risks defined in prior domain i.e. risk assessment), *information and communication* (create reporting processes that help in assessment of the technology environment), *monitoring*

(assessment of the quality of a company's internal control over time). COSO and COBIT frameworks are widely used as guidelines for Sarbanes-Oxley compliance, systems audit in organizations and also for information technology governance purposes.

Most of the best practices are based on "gut feel", experiences of a few and are atheoretic in nature. The guidelines thus provided are mechanistic and have "one size fits all" orientation. The frameworks are also broad in nature and do not specifically address issues regarding internal controls for security. Control is a central problem in the study of hierarchical organization as opportunities for distortion and misalignment of goals are rich (Ouchi, 1978). Bulk of the research in the controls area is technical and has a formal scope and targeted more at behavioral and output.

In summary, the research stream in controls area is characterized by three problems: lack of theoretical basis for defining internal control objectives, inadequate emphasis on individual values in control design and lack of research in information systems security domain about internal control design. This paper fills this gap by suggesting value focused thinking as a means to incorporate individual values into control objectives and provides a theoretical framework of means and fundamental objectives for internal controls in information systems.

3 THEORY AND METHODOLOGY

The theoretical basis for this study is Catton's (1952) value Theory and Keeney's (1992) value focused thinking. This section provides a description of the theory and the methodology and illustrates the use of the methodology for this specific study.

3.1 Value Theory

According to Catton (1952) an individual's preferential behavior shows certain regularities and this pattern can be attributed to some standard or code, which persists through time. Values provide a basis by which people can order their intensities of desiring various desiderata (something desirable). Based on available choices, people make preferences grounded in their values. In an organizational context, knowledge of such preferences of individuals provides a context for managerial decision-making. Keeney (1992) argues that values are guiding principles to evaluate the desirability of a particular consequence. "Values are what we care about and they should be the driving force for our decision making (Keeney, 1992, pp. 3)".

Value is not a property of an object but is a quality of relationship (Catton, 1952, pp. 108). A person's desire for something under a given situation depends on "selective perception" of that person. Selective perception directs valuation by substituting final goals with other intermediary goals i.e. a goal may be pursued in order to attain some higher ultimate goals. Thus the nature of the major goals of accepted by individuals together with notions of ways in which these goals might be affected by future events, are the determinants of values of people. Value Theory provides a theoretical platform to affirm that values are important for decision making and incorporating values in developing decision objectives helps individuals accept the results of such decisions.

3.2 Value Focused Approach

Keeney (1992) suggests that value focused thinking is a better way of making decisions especially if there are many subjective interpretations involved. Values are more fundamental to a decision context than the available alternatives. But in common practice, decision-making usually focuses on the choice among existent alternatives. The relative desirability of the consequences can be best understood if the values of the decision maker are reflected in the decision.

To create internal control objectives from the individual values, this study uses a three-step procedure as proposed by Keeney (1992). These steps are:

Develop a comprehensive list of personal values underlying the problem being explored: Probing is required on the part of the researcher to elicit the underlying values of respondents. The process of identifying the values begins with interviewing people. The interview is semi structured, with emphasis on exploring the respondent's values through innovative ways such as scenario building, illustrative examples or story telling. A guiding definition is provided about the research context and direct questions about values are avoided. Values are difficult to surface and more difficult to express explicitly. The personal values surfaced through the interview session are listed.

Change the values enlisted to a common form: These common denominators give rise to values. Raw values are identified from the interview data and converted into common form. To convert the values into objectives, a verb is added to these values. The values that are listed are objects and ways to adding a directional preference converts them to an objective. The verb form of the values thus created could be termed as the objective of that object. An objective has three features: a decision context, an object and a direction of preference (Keeney, 1992).

Classify the objectives as means and fundamental and create a framework of means and fundamental objectives for the decision context: In the final step of this process, a means-fundamental objective framework is created. Fundamental objectives are dependent on other objectives to achieve the desired result in a decision-making situation. Fundamental objectives are objectives important in their own right in a decision making process. The clustering of objectives into means and fundamental genre is primarily done by performing a "why is this important" (WITI) test for each of the objectives (Keeney, 1992). Classification of all the objectives formed is done and all the objectives clusters are divided into two categories, "means" or "fundamental" and a means-fundamental network is developed.

4 DEVELOPING THE THEORETICAL FRAMEWORK: MEANS-FUNDAMENTAL OBJECTIVES FOR INTERNAL CONTROLS

This section demonstrates the use of a three-step methodology for value-focused assessment. The values of respondents identified during the process are structured to create a theoretical framework for internal control objectives for information systems security.

Develop a list of values: In this study, 52 interviews were conducted in a broad cross section of industries. The average duration for each interview was about an hour. The researchers contacted the participants. Interviewees had an average work experience of ten years in information technology area and more than seven years of exposure to information systems security related work. The respondents belong to the following industries: Banking, insurance, healthcare, manufacturing, consulting and auditing. The nature of job description included chief information officer, senior security administrator, systems auditor, consultants and technical support executive. The consolidated data from all the interviews showed a list of 276 values with overlaps. Removing the duplicate values, a list of 195 values was created. Table 3 shows the list of means values developed in this study.

Change values into objectives: From the list of values, 68 objectives were developed. The researchers did the creation of objectives intuitively in an iterative manner, where the emerging themes from the values were captured and labelled conceptually.

Classify the objectives as means and fundamental: Differentiation of objectives into means and fundamentals is critical to making informed decisions about a decision context (Dhillon and Torkzadeh, 2006). Structuring of the objectives is very important for understating what individuals care about in a given context. This step calls for conceptually differentiating between means and fundamental objectives.

Applying the WITI test, categories of means and fundamental objectives are created and their interrelationships were established. For example, objective such as "enhance responsibility for actions" leads to another objective "promote single line of command" which in turn helps in "enhance clarity in business processes". Each of these controls, through important in its own right, contribute in achieving the fundamental objective of "Increase ability to link controls with organizational authority structures". An objective is fundamental since it helps in achieving the overall objective of maximizing effectiveness of internal controls and creating a better control environment. The application of WITI test to all the objectives resulted in seven fundamental and eighteen means objectives for internal controls. Table 4 shows the list of fundamental objectives for internal controls in information systems security.

Table 2. Means Objectives Related to Internal Controls for Information Systems Security

Ensure senior management involvement in designing controls *Example: Encourage senior management education about controls*	Provide training *Example: Encourage specialized training about control*
Educate employees about controls *Example: Explain the consequences of actions*	Promote single line of command *Example: Centralize control management*
Enhance responsibility for actions *Example: Create an environment of ownership*	Encourage control consciousness *Example: Evaluate periodically the knowledge about control*
Communicate the intention and purpose of controls *Example: Explain the scope of the control*	Ensure Audit efficacy of controls *Example: Ensure periodic assessment of controls*
Explain enterprise need for controls *Example: Establish the importance of control environment*	Enhance ability to use the information for intended purpose *Example: Encourage the use of the knowledge in daily practice*
Enforce censure *Example: Ensure deterrent activities*	Enhance positive perception about controls *Example: Explain importance of controls*
Provide sense of direction *Example: Explain organizational objectives and goals*	Increase ability to develop good policies *Example: Communicate the role of policies for strong controls*
Ensure controls as part of policy *Example: Create control around the policies*	Enhance clarity of business processes *Example: Educate deeply about the business processes*
Develop ability to periodically review controls *Example: Ensure effectiveness of controls during change in roles*	Enhance knowledge about controls *Example: Explain the intricacies of each control*

Table 3. Fundamental Objectives Related to Internal Controls for Information Systems Security

Increase ability to strategize controls *Example: Evaluate organization's security objectives*	Maximize awareness about controls *Example: Create control conscious culture*
Increase ability to link controls with organizational authority structures *Example: Ensure accountability in management structures*	Enhance ability to evaluate business processes periodically *Example: Ensure flexibility in defining control*
Ensure technical architecture review *Example: Emphasize on technical requirement of controls*	Increase clarity in role definitions *Example: Established boundaries in job definitions*
Ensure regulatory compliance *Example: Ensure substantive inputs from laws*	

5 DISCUSSION

The means and fundamental objectives developed in this research are organizationally grounded control objectives for information systems. Based on the extant literature on controls, we present the insights drawn from this study.

When the scope of control is technical in nature and requirements are precise, various technical solutions are instituted in the business process targeted at different levels. Controls such as document design, architectural plan, authentication mechanism, firewalls and biometrics are instituted. There is an overwhelming emphasis on technical controls in research where controls are synonymous to access or authentication management. A majority of the respondents felt that complete reliance only on technical controls cannot provide the intended security governance structure. Discussing the intricacies of having good access control mechanism in place, one of the respondents, a senior systems auditor observed; "*Appropriateness of the access is a very high level generic control. The specific tool that is used to ensure right access may be very different for organizations"*. In the research literature, there is a great emphasis on technical controls for information systems security governance (Siponen, 2001, 2006; Thompson et al, 2003). The respondents unanimously agreed on the importance of technical controls such as access mechanisms, authentication models, encryption techniques and firewalls. But a need to go beyond such controls into more fundamental ways of dealing with threats was felt. This insight from our results seem conceptually consistent with the state of affairs in information systems security research, where there is a significant emphasis on technical aspects of security governance rather than organizational or informal aspects (Baskerville, 1993; Dhillon & Backhouse, 2001; Straub & Welke, 1998). Since security governance is perceived more of a technical than organizational issue (Dhillon and Torkzadeh, 2006), there is a greater thrust in developing technical controls for security governance. One of our fundamental objectives "Ensure technical architecture review" is supported by other means objectives such as "Ensure audit efficacy of controls" and "Explain enterprise need for controls". But technical controls, on its own, are incapable of providing an overall sound governance structure to an organization. A value assessment of the people across industries shows that creating awareness about controls, providing specialized controls training

and communicating the intended use of controls goes a long way in ensuring that controls are effective.

The second dimension of control mode is formal in scope. The control mechanism based on the formal level of organization uses rules, conformity and incentives as ways of controlling the task environment. Bureaucratic controls based on various stages of business process (input, behavioral, output) incorporate risk assessment models, security investment decisions, policies, procedures, compliance and governance issues. Our fundamental objectives such as "Ability to strategize controls", "Enhance ability to evaluate business processes periodically" and "Ensure regulatory compliance" actually emphasize efficient bureaucratic controls for security governance.

Research literature in controls for security identifies the importance of security policies in creation of effective controls (Ward and Smith, 2002; Moultan and Cole, 2003; Thompson and von Solms, 2005). Many of our respondents emphasized the importance of having good security policies for creating right controls. One of the respondents commented; "*I just tell the audit clients, if you just even go to your policies and try to implement them via controls so that you can answer some of the security questions, you will be far ahead"*.

Our results show that it is important to concentrate on the organizational controls as well for better security governance. Some of our mean objectives such as "Enhance clarity of business processes", "Ensure Audit efficacy of controls", "Provide training", "Enforce censure" and "Develop ability to periodically review controls" point towards the encompassing role of bureaucratic controls in overall control management for security. This finding is consistent with research in organizational aspects of controls where an emphasis is put on effective security governance structures for overall management of control environment **(**Rezmierski et al, 2004; Whitman, 2003; Warkentin, and Johnston, 2006). But there is a sense of caution in being overly dependent on bureaucratic control and missing the opportunity to communicate informally about the role of such management level activities. Compliance with regulations, for instance, can be used for improving fundamentally the control structure or could just be another checklist for the management. The values of respondents show that there should be involvement of senior management into designing and implementing controls such that a "direction" is provided to the organization. Bureaucratic controls are good if the organizational objectives are communicated effectively "top down" and there is no transmission loss. The communication can be achieved through effective policies, procedures, senior management involvement, training, and creating awareness about controls.

The third group of controls is informal in nature and enforces the internal controls through development of shared goals and alignment of individual and organizational objectives. Research in information systems security emphasizes the importance individual values, behavior, beliefs and organizational culture in improving the security effectiveness (Magklaras and Furnell, 2005; Stanton et at, 2005; McHugh and Deek, 2005; Loch and Conger, 1996). Our findings are consistent with the stream of research in information systems security that emphasizes the impact of informal aspects of security governance. To have a better representation of informal aspects of security in governance structures, efforts in developing more clan type of control mode is warranted. Informal controls act at all stages of business process and contribute to the control environment by emphasizing the importance of values, behavior, motivations, trust and sense of ownership. There is a lack of research in internal controls for information systems security seriously about the informal aspects of controls. Our data shows that controls should incorporate the values, beliefs and individual inputs, to ensure effectiveness of any type of control. One of the interviewees said; "*Controls must focus on what people think are good, it usually starts with people; it need not be technology side"*. The security controls being popularly used in organizations lack the perspective of the employees who are actually going to implement the

controls. This causes a gap between management's intended reason for instituting controls and employee's interpretation of the controls. As one of our respondent observed; "*Nothing can derail a security initiative quicker if people feel you are not being responsible. If you take control away from people and try to impose, it makes people jump their hoops. It is really not a technology business, its people business that has a lot to do with technology. I am constantly trying to reinforce this"*.

Our research shows that there is much more to successfully defining internal control objectives for information systems security than just getting the technology right and creating administrative policies and procedures around it. These aspects are important too. Creating a control conscious environment and aligning individual goals of the employees with the organizational security goals is important as well. Our findings are corroborated by the research findings in information systems security domain where a lack of informal security environment is felt (Adams and Sasse, 1999; Schultz, 2002). Some of our fundamental objectives such as "Increase ability to link controls with organizational authority structures", "Increase clarity in role definitions" and "Maximize awareness about controls" indicate the importance of incorporating people's view into defining control objectives. Some of our means objectives such as "Enhance positive perception about controls", "Enhance knowledge about controls" and "Enhance ability to use the information for intended purpose" show that employees should be explained the benefits of controls and should be encouraged to use the knowledge in daily practice.

The new insight that this research provides is that instituting informal controls is important for effective security governance in an organization. If the security control objectives are aligned with individual's objectives, the organization would be more secure. Our results also establish a link between effectiveness of internal controls and organization's security initiatives. There have been many calls in past to claim that internal controls are important for organization's overall security (Dhillon, 2001; Warkentein, 2006), but there have been no evidence to support such assertions. Our study shows the success of security governance programs are related to the effectiveness of internal controls. This is a contribution to the field of information systems security and control literature. Theoretically, this research provides a list of means and fundamental for defining internal control objectives for information systems security. It provides objectives, grounded in organizational values about security controls, which can be used for effective controls design. This makes a theoretical contribution to information systems discipline. For practitioners in the real world, this framework provides guidelines about the importance of incorporating employee's perspective into control design for better results of security governance initiatives.

6 CONCLUSION

This paper examines a relatively unexplored area in information systems research. This research provides a theoretical framework for defining internal control objectives for information systems security in an organization. The objectives, grounded in data, provide the basis for designing effective governance structure. Value focused thinking provides decision objectives that are more effective in the long run that objectives based on alternative focused thinking (Keeney, 1992). This paper incorporates value focused thinking to develop the control objectives for information systems security. The findings suggest that clam based control mechanisms are important for overall effectiveness of internal controls. There is significant contribution because there are limited theoretical models to guide the formation of control objectives for information systems security governance. The findings also suggest that control mechanisms such as technical or formal, fall short, if the informal aspects of control environment are not taken into account.

References

Adams, A., and Sasse, M.A. "Users are not the enemy. Association for Computing Machinery," *Communications of the ACM* (42:12) 1999, pp 40-46.

Aeran, A. "Comprehensive overview of Insider Threats and their Controls," Royal Holloway, University of London, MS thesis, 2006, pp. 1-68.

Bodin, L.D., Lawrence A. Gordon, and Loeb, M.P. "Evaluating Information Security Investments Using the Analytic Hierarchy Process," *Communications of the ACM* (48:2) 2005, pp 79-83.

Cardinal, L.B., Sitkin, S.B., and Long, C.P. "Balancing and Rebalancing in the Creation and Evolution of Organizational Control," *Organization Science* (15:4) 2004, pp 411-431.

Catton, W.R. "Exploring Techniques for Measuring Human Values," *American Sociological Review* (19:1) 1954, pp 49-55.

Catton, W.R. "A Retest of the Measurability of Certain Human Values," *American Sociological Review* (21:3) 1956, pp 357-359.

Catton, W.R. "A Theory of Value," *American Sociological Review* (24:3) 1959, pp 310-317.

Choy, M., Leong, H.V., and Wong, M.H. "Disaster Recovery Techniques for Database Systems," *Communications of the ACM*) 2000, pp 272-280.

Dhillon, G. "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." Computers & Security 20(2): 165-172.

Dhillon, G., and Backhouse, J. "Information System Security Management in the New Millennium," *Communications of the ACM* (43:7) 2000, pp 125- 128.

Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," *Information Systems Journal* (16:3) 2006, pp 293-314.

Eisenhardt, K. "Control:Organizational and Economic Approaches," *Management Science* (31:2) 1985, pp 134-149.

Galloway, D.J. "Control models in perspective," *The Internal Auditor* (51:6) 1994, pp 46-52.

Gordon, L.A., and Loeb, M.P. "Using Information Security as a Response to Competitor Analysis Systems," *Communications of the ACM* (44:9) 2001, pp 70-75.

Hofmann, T. "Latent Semantic Models for Collaborative Filtering," *ACM Transactions on Information Systems* (22:1) 2004, pp 89-115.

Keeney, R. *Value-focussed thinking: a path to creative decisionmaking* Harvard University Press, Cambridge:Massachusetts, 1992.

Keeney, R. "The Value of Internet Commerce to the Customer," *Management Science* (45:4) 1999, pp 533-542.

Kirsch, L.J. "Deploying Common Systems Globally: The Dynamics of Control," *Information Systems Research* (15:4) 2004.

Kirsch, L.J., Sambamurthy, V., Ko, D.-G., and Purvis, R.L. "Controlling Information Systems Development Projects:The View from the Client " *Management Science* (48:4) 2002, pp 484-498.

Klein, H.J. "An Integrated Control Theory Model of Work Motivation," *Academy of Management Review* (14:2) 1989, pp 150-172.

Loch, K., and Conger, S. " Evaluating Ethical Decision Making and Computer Use," *Communications of the ACM* (39:7), July 1996 1996, pp 74-83.

Magklaras, G., and Furnell, S. "A preliminary model of end user sophistication for insider threat prediction in IT systems," *Computers & Security* (24) 2005, pp 371-380.

McHugh, J., and Deek, F. "An incentive system for reducing Malware Attacks," *Communications of the ACM* (48:6), June 2005 2005, pp 94-99.

Ouchi, W.G. "The Relationship between Organizational Structure and Organizational Control," *Administrative Science Quarterly* (22:1) 1977, pp 95-113.

Ouchi, W.G. "A Conceptual Framework for the Design of Organizational Control Mechanisms," *Management Science* (25:9) 1979, pp 833-848.

Ouchi, W.G. "Markets, Bureacracies and Clan," *Administrative Science Quarterly* (25:1) 1980, pp 129-141.
Schultz, E. "A framework for understanding and predicting insider attacks," in: *Compsec* London, 2002.
Siponen, M. "Five Dimensions of Information Security Awareness," *Computers and Society*:June) 2001, pp 24-29.
Snell, S.A. "Control Theory in Strategic Human Resource Management: The Mediating Effect of Administrative Information," *Academy of management Journal* (35:2) 1992, pp 292-327.
Stanton, J., and Stam, K. " Analysis of end user security behaviors," *Computers & Security* (24) 2005, pp 124-133.
Straub, D. "Coping with systems risk: security planning models for management decision making.," *MIS Quarterly*
(22:8) 1998, pp 441-465.
Straub, D., and Welke, R. "Coping with systems risk: security planning models for management decision making.," *MIS Quarterly* (22:8) 1998, pp 441-465.
Von Solms, B. "Corporate Governance and Information Security," *Computers & Security* (20:3) 2001, pp 215-218.
Ward, P., and Smith, C. "The Development of Access Control Policies for Information Technology Systems," *Computers & Security* (21:4) 2002, pp 356-371.
Warkentin, M., and Johnston, A. *IT Security Governance and Centralized Security Controls* Idea Group Publishing, Hershey, P.A, 2006.
Whitman, M. "Enemy at the Gate: Threats to Information Security," *Communications of the ACM* (46:8) 2003, pp 91-95.